UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/728,701	12/01/2000	Mark Muhlestein	103.1056.01	4879

22883 7590 01/07/2005

SWERNOFSKY LAW GROUP PC
P.O. BOX 390013
MOUNTAIN VIEW, CA 94039-0013

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 01/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/728,701	MUHLESTEIN, MARK	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 August 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15,18-34,37-43,45,57,59-62,74-77,79and 91* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15,18-34,37-43,45,57,59-62,74-77,79 and 91* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on August 2, 2004. The original application contained claims 1 – 91. Per the received amendment, claims 1,4,11,12,18-21,23,30,31,37-41,57,61,74,75,79, and 91 have been amended and claims 16,17,35,36,44,46-56,58,63-73,78, and 80-90 have been cancelled. Presently pending claims are 1-15,18-34,37-43,45,57,59-62,74-77, 79 and 91.

Response to Arguments

2. Applicant's arguments filed on August 2, 2004 have been fully considered but they are not considered persuasive because of the following reasons:

Regarding currently amended claims 1, 21, 57 and 91, the applicant argues that the cited prior art, Tso et al. (U.S. Patent 6,088,803) and Bates et al. (U.S. Patent 6,721,721) does not teach, "content encryption." These arguments are not found persuasive in view of the cited prior art Bates. Bates teaches "any packets sent by the plugin 29 to virus check controller 44 are encrypted" (column 14 lines 62 – 67). The applicant argues that the encryption of "virus status information" is not considered "content encryption" and therefore Bates' encryption scheme cannot be used in conjunction with Tso to encrypt the object that was requested and scanned for viruses.

However, the Examiner maintains that "content encryption" is analogous to encrypting the "virus status information" as both are just data. Also, encrypting data objects was well-known in the art at the time of the Applicant's invention, and it would have been obvious to encrypt the object before sending it over a communications network because, as according to Bates, it would "prevent a malicious party from attempting to corrupt the...information" (column 15 lines 1 – 8). Regarding amended independent claims 40 and 74 and dependent claims 6 and 25, the Applicant argues that the cited prior art does not teach nor suggest non-uniform memory access (NUMA). This argument is not found persuasive. Bates teaches a virus-scanning environment wherein the scanning device is one of a cluster of scanning devices that can be used to scan for viruses (column 3 lines 38 – 55, column 4 lines 50-55, column 8 lines 16 – 29). It was well-known in the art that NUMA-like performance can be achieved using clusters, with nodal latency being the only issue. However, NUMA is a memory architecture that is commonly used in multiprocessors like the ones used in the cited prior art Bates. However, it was well-known at the time of invention that the NUMA architecture overcomes scalability issues when many CPU's are involved. Therefore, it would have been obvious to use the NUMA architecture in the cluster architecture of Bates to reduce the number of CPUs competing for access to a shared memory bus, and henceforth, increasing the speed that each of the packets are processed. Regarding dependent claims 9 and 28, the Applicant argues that the cited prior art does not teach nor suggest that the processing cluster is performed in a round robin fashion. Bates discloses a cluster of scanning devices which process files as they arrive (column

3 lines 38 – 55, column 4 lines 50-55, column 8 lines 16 – 29). Bates does not explicitly state that round robin scheduling is used, however, it was well-known in the art at the time of invention that round-robin scheduling is used so that each process can take turns processing an incoming file. It is obvious that any one of many scheduling schemes can be applied to the processing cluster of Bates, but to allow the fair sharing of the processing of each incoming packet, it is obvious that round-robin scheduling can be applied. Accordingly, the rejection for the pending claims 1-15,18-34,37-43,45,57,59-62,74-77,79 and 91 are respectfully maintained as given below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-15,18-34,37-43,45,57,59-62,74-77, 79 and 91 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tso et al. (U.S. Patent 6,088,803) in view of Bates et al. (U.S. Patent 6,721,721).

Regarding claim 1, Tso discloses:

A method for operating a filer including the steps of:

receiving at a first location a request from a user for an object (Figure 2 item 20, column 2 lines 62 - 67);

responding to said request, wherein said step of responding includes delivery of a response to said user (Figure 2 item 60, item 70, column 3 lines 1 – 10).

Tso does not explicitly teach processing said request at a second location, wherein said step of processing includes encrypting said object. Bates teaches "any packets sent by the plugin 29 to virus check controller 44 are encrypted" (column 14 lines 62 – 67). Also, encrypting data objects was well-known in the art at the time of the Applicant's invention, and it would have been obvious to encrypt the object before sending it over a communications network because, as according to Bates, it would "prevent a malicious party from attempting to corrupt the...information" (column 15 lines 1 – 8).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Tso discloses:

The method of claim 1 wherein said request is in an electronic form (column 2 lines 62 – 67).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Tso discloses:

The method of claim 1, wherein said object is a file (column 2 line 62 – column 3 line 5).

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Tso discloses:

The method of claim 3. Tso does not explicitly describe the use of a processing cluster to process files and generate reports. Bates teaches creating an access path to

a processing cluster, processing a file in the processing cluster, and generating a scan report that is responsive to the processing of the file in the processing cluster (column 3 lines 38 – 55, column 4 lines 50-55, column 8 lines 16 – 29). Both Bates and Tso pertain to methods of virus scanning and reporting and are therefore analogous arts. Bates states that using multiple computers to scan for virus information permits "the responsibility for generating virus status information, as well as the processing horsepower required to generate the virus status information, to be allocated among the multiple computers" (column 3 lines 38 – 55). Further, Bates states, "by distributing the virus checking responsibilities in this manner, a comparatively greater volume of virus status information may be generated and/or the timeliness of updates to existing virus status information may be improved" (column 3 lines 51 – 55). Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Tso with the cluster of virus scanning devices of Bates to achieve the benefits of reduction of processing power at the scanning device, diversifying the source of virus status information, and as a result, increasing the timeliness of virus status information and the volume of virus status information.

Claim 5 is rejected as applied above in rejecting claim 4. Tso does not explicitly discloses the method of creating an access path including sending the ID and path of said file from said filer to said processing cluster. Bates discloses sending the ID and the path of said file from said filer to said processing cluster (column 6 line 65 – column 7 line 19). It would have been obvious to send the ID and path of the file to the

processing cluster following the logic used above in rejecting the parent claims. Also, it would have been obvious since the files are stored in a database along with results of virus scans in both the inventions of Tso and Bates, that a ID is needed to identify the file and its resultant virus scan in a database.

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Tso discloses:

The method of claim 5, wherein said step of sending is accomplished using non-uniform memory access (column 5 lines 1 – 63).

Claim 7 is rejected as applied above in rejecting claim 5. Furthermore, Tso discloses:

The method of claim 5, wherein said step of sending is accomplished using a communications network (column 5 lines 1 – 63).

Claim 8 is rejected as applied above in rejecting claim 5. Furthermore, Tso discloses:

The method of claim 5, wherein said step of sending is accomplished using a direct connection (column 5 lines 1 – 63).

Claim 9 is rejected as applied above in rejecting claim 4. Tso does not explicitly describe the use of a round robin processing method in a cluster. Bates teaches processing files in a processing cluster using a round robin method (column 3 lines 38 – 55, column 4 lines 50-55, column 8 lines 16 – 29). Both Bates and Tso pertain to methods of virus scanning and reporting and are therefore analogous arts. Bates states

that using multiple computers to scan for virus information permits "the responsibility for generating virus status information, as well as the processing horsepower required to generate the virus status information, to be allocated among the multiple responsibilities in this manner, a comparatively greater volume of virus status information may be generated and/or the timeliness of updates to existing virus status information may be improved" (column 3 lines 51 – 55). computers" (column 3 lines 38 – 55). Further, Bates states, "by distributing the virus checking Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Tso with the round robin processing cluster of virus scanning devices of Bates to achieve the benefits of reduction of processing power at the scanning device, diversifying the source of virus status information, and as a result, increasing the timeliness of virus status information and the volume of virus status information.

Claim 10 is rejected as applied above in rejecting claim 4. Furthermore, Tso discloses:

Processing said file in parts. Tso does not explicitly disclose the file is processed in parts by more than one device in said processing cluster. Bates teaches processing files in a processing cluster (column 3 lines 38 – 55, column 4 lines 50-55, column 8 lines 16 – 29). Both Bates and Tso pertain to methods of virus scanning and reporting and are therefore analogous arts. Bates states that using multiple computers to scan for virus information permits "the responsibility for generating virus status information, as well as the processing horsepower required to generate the virus status information, to be allocated among the multiple computers" (column 3 lines 38 – 55). Further, Bates

states, "by distributing the virus checking responsibilities in this manner, a comparatively greater volume of virus status information may be generated and/or the timeliness of updates to existing virus status information may be improved" (column 3 lines 51 – 55). Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Tso with the processing cluster of virus scanning devices of Bates to process the file in parts and achieve the benefits of reduction of processing power at the scanning device, diversifying the source of virus status information, and as a result, increasing the timeliness of virus status information and the volume of virus status information.

Claim 11 is rejected as applied above in rejecting claim 4. Furthermore, Tso discloses:

The method of claim 4, wherein all files stored on said filer are encrypted in a logical continuous manner (column 3 lines 1 – 54).

Claim 12 is rejected as applied above in rejecting claim 4. Furthermore, Tso discloses:

The method of claim 4, wherein said scan report contains a set of status data relating to said processing of file (column 3 lines 39 – 54).

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Tso discloses:

The method of claim 12, wherein said status data includes at least one data element identifying the presence or non-presence of a virus in said file (column 3 lines 39 – 54).

Claim 14 is rejected as applied above in rejecting claim 13. Furthermore, Tso discloses:

The method of claim 13, wherein said report is transferred to said filer (Figure 3 item 200, column 3 lines 48 – 54).

Claim 15 is rejected as applied above in rejecting claim 14. Furthermore, Tso discloses:

The method of claim 14, wherein said report is stored in a first database (column 5 lines 1 – 26).

Claim 18 is rejected as applied above in rejecting claim 3. Furthermore, Tso discloses:

The method of claim 3, wherein said delivery of a response is said file (Figure 2 item 60, item 70, column 3 lines 1 – 10).

Claim 19 is rejected as applied above in rejecting claim 3. Furthermore, Tso discloses:

The method of claim 3, wherein said delivery of a response includes modification to said user that said file is unavailable (Figure 3 item 200, column 3 lines 48 – 54).

Claim 20 is rejected as applied above in rejecting claim 4. Furthermore, Tso discloses:

The method of claim 4, wherein said step of responding to said request includes sending said user a copy of said report (Figure 3 item 200, column 3 lines 48 – 54).

Regarding claim 21, Tso discloses:

An apparatus for operating a filer including:

means for receiving at a first location a request from a user for an object (Figure 2 item 20, column 2 lines 62 - 67);

means for processing said request at a second location, wherein said means for processing includes means for encrypting said object

means for responding to said request, wherein said means for responding includes delivery of a response to said user (Figure 2 item 60, item 70, column 3 lines 1 – 10).

Tso does not explicitly teach means for processing said request at a second location, wherein said means for processing includes means for encrypting said object. Bates teaches "any packets sent by the plugin 29 to virus check controller 44 are encrypted" (column 14 lines 62 – 67). Also, encrypting data objects was well-known in the art at the time of the Applicant's invention, and it would have been obvious to encrypt the object before sending it over a communications network because, as according to Bates, it would "prevent a malicious party from attempting to corrupt the...information" (column 15 lines 1 – 8).

Claim 22 is rejected as applied above in rejecting claim 21. Furthermore, Tso discloses:

The apparatus of claim 21, wherein said object is a file (column 2 line 62 – column 3 line 5).

Claim 23 is rejected as applied above in rejecting claim 22. Furthermore, Tso discloses:

The apparatus of claim 22. Tso does not explicitly describe the use of a processing cluster to process files and generate scan reports. Bates teaches creating an access path to a processing cluster, processing a file in the processing cluster, and generating a scan report that is responsive to the processing of the file in the processing cluster (column 3 lines 38 – 55, column 4 lines 50-55, column 8 lines 16 – 29). Both Bates and Tso pertain to methods of virus scanning and reporting and are therefore analogous arts. Bates states that using multiple computers to scan for virus information permits "the responsibility for generating virus status information, as well as the processing horsepower required to generate the virus status information, to be allocated among the multiple computers" (column 3 lines 38 – 55). Further, Bates states, "by distributing the virus checking responsibilities in this manner, a comparatively greater volume of virus status information may be generated and/or the timeliness of updates to existing virus status information may be improved" (column 3 lines 51 – 55). Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Tso with the cluster of virus scanning devices of Bates to achieve the benefits of reduction of processing power at the scanning device, diversifying the source of virus status information, and as a result, increasing the timeliness of virus status information and the volume of virus status information.

Claim 24 is rejected as applied above in rejecting claim 23. Tso does not explicitly discloses the method of creating an access path including sending the ID and path of

said file from said filer to said processing cluster. Bates discloses sending the ID and the path of said file from said filer to said processing cluster (column 6 line 65 – column 7 line 19). It would have been obvious to send the ID and path of the file to the processing cluster following the logic used above in rejecting the parent claims. Also, it would have been obvious since the files are stored in a database along with results of virus scans in both the inventions of Tso and Bates, that a ID is needed to identify the file and its resultant virus scan in a database.

Claim 25 is rejected as applied above in rejecting claim 24. Furthermore, Tso discloses:

The apparatus of claim 24, wherein said step of sending is accomplished using non-uniform memory access (column 5 lines 1 – 63).

Claim 26 is rejected as applied above in rejecting claim 24. Furthermore, Tso discloses:

The apparatus of claim 24, wherein said step of sending is accomplished using a communications network (column 5 lines 1 – 63).

Claim 27 is rejected as applied above in rejecting claim 24. Furthermore, Tso discloses:

The apparatus of claim 24, wherein said sending is accomplished using a direct connection (column 5 lines 1 – 63).

Claim 28 is rejected as applied above in rejecting claim 23. Tso does not explicitly describe the use of a round robin processing method in a cluster. Bates teaches

processing files in a processing cluster using a round robin method (column 3 lines 38 – 55, column 4 lines 50-55, column 8 lines 16 – 29). Both Bates and Tso pertain to methods of virus scanning and reporting and are therefore analogous arts. Bates states that using multiple computers to scan for virus information permits "the responsibility for generating virus status information, as well as the processing horsepower required to generate the virus status information, to be allocated among the multiple computers" (column 3 lines 38 – 55). Further, Bates states, "by distributing the virus checking responsibilities in this manner, a comparatively greater volume of virus status information may be generated and/or the timeliness of updates to existing virus status information may be improved" (column 3 lines 51 – 55). Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Tso with the round robin processing cluster of virus scanning devices of Bates to achieve the benefits of reduction of processing power at the scanning device, diversifying the source of virus status information, and as a result, increasing the timeliness of virus status information and the volume of virus status information.

Claim 29 is rejected as applied above in rejecting claim 23. Furthermore, Tso discloses:

Processing said file in parts. Tso does not explicitly disclose the file is processed in parts by more than one device in said processing cluster. Bates teaches processing files in a processing cluster (column 3 lines 38 – 55, column 4 lines 50-55, column 8 lines 16 – 29). Both Bates and Tso pertain to methods of virus scanning and reporting

and are therefore analogous arts. Bates states that using multiple computers to scan for virus information permits "the responsibility for generating virus status information, as well as the processing horsepower required to generate the virus status information, to be allocated among the multiple computers" (column 3 lines 38 – 55). Further, Bates states, "by distributing the virus checking responsibilities in this manner, a comparatively greater volume of virus status information may be generated and/or the timeliness of updates to existing virus status information may be improved" (column 3 lines 51 – 55). Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Tso with the processing cluster of virus scanning devices of Bates to process the file in parts and achieve the benefits of reduction of processing power at the scanning device, diversifying the source of virus status information, and as a result, increasing the timeliness of virus status information and the volume of virus status information.

Claim 30 is rejected as applied above in rejecting claim 23. Furthermore, Tso discloses:

The apparatus of claim 23, wherein all files stored on said filer are encrypted in a logical continuous manner (column 3 lines 1 – 54).

Claim 31 is rejected as applied above in rejecting claim 23. Furthermore, Tso discloses:

The apparatus of claim 23, wherein said report contains a set of status data relating to said processing of said file (column 3 lines 39 – 54).

Claim 32 is rejected as applied above in rejecting claim 31. Furthermore, Tso discloses:

The apparatus of claim 31, wherein said status data includes at least one data element identifying the presence or non-presence of a virus in said file (column 3 lines 39 – 54).

Claim 33 is rejected as applied above in rejecting claim 31. Furthermore, Tso discloses:

The apparatus of claim 31, wherein said report is transferred to said filer (Figure 3 item 200, column 3 lines 48 – 54).

Claim 34 is rejected as applied above in rejecting claim 33. Furthermore, Tso discloses:

The apparatus of claim 33, wherein said report is stored in a first database (column 5 lines 1 – 26).

Claim 37 is rejected as applied above in rejecting claim 22. Furthermore, Tso discloses:

The apparatus of claim 22, wherein said delivery of a response is delivery of said file (Figure 2 item 60, item 70, column 3 lines 1 – 10).

Claim 38 is rejected as applied above in rejecting claim 22. Furthermore, Tso discloses:

The apparatus of claim 22, wherein said delivery of a response includes delivery of notification to said user that said file is unavailable (Figure 3 item 200, column 3 lines 48 – 54).

Claim 39 is rejected as applied above in rejecting claim 23. Furthermore, Tso discloses:

The apparatus of claim 23, wherein said responding to said request includes sending said user some portion of said report (Figure 3 item 200, column 3 lines 48 – 54).

Regarding claim 40, Tso discloses:

A method of attempting to provide virus protection in a client-server environment, comprising the steps of:

receiving a request at a server for a file (Figure 2 item 20, column 2 lines 62 - 67);

sending, from the server, an identifier for the file to a scanning device that scans the file for viruses (Figure 2 item 40, column 2 lines 38 – 44, column 3 lines 1 - 10);

receiving, at the server, an indication from the scanning device as to whether or not the file is safe to send from the server (Figure 3 item 200, column 3 lines 48 – 54); and

responding to the request by sending the file if the indication is that the file is safe to send (Figure 2 item 60, item 70, column 3 lines 1 – 10).

Tso does not explicitly disclose that the communication between the server and the cluster of scanning devices is performed using non-uniform memory access. . Bates teaches a virus-scanning environment wherein the scanning device is one of a cluster of scanning devices that can be used to scan for viruses (column 3 lines 38 – 55,

column 4 lines 50-55, column 8 lines 16 – 29). It was well-known in the art that NUMA-like performance can be achieved using clusters, with nodal latency being the only issue. However, NUMA is a memory architecture that is commonly used in multiprocessors like the ones used in the cited prior art Bates. However, it was well-known at the time of invention that the NUMA architecture overcomes scalability issues when many CPU's are involved. Therefore, it would have been obvious to use the NUMA architecture in the cluster architecture of Bates to reduce the number of CPUs competing for access to a shared memory bus, and henceforth, increasing the speed that each of the packets are processed.

Claim 41 is rejected as applied above in rejecting claim 40. Furthermore, Tso discloses:

A method as in claim 40, wherein the scanning devices indicate that the file is safe to send if the scanning devices determine that the file is not infected with any viruses (Figure 3 item 200, column 3 lines 48 – 54).

Claim 42 is rejected as applied above in rejecting claim 40. Furthermore, Tso discloses:

A method as in claim 40, wherein the request is received from and the file is sent to a client device (Figure 2 item 60, item 70, column 3 lines 1 – 10).

Claim 43 is rejected as applied above in rejecting claim 40. Furthermore, Tso discloses:

A method as in claim 40, wherein the server is a web server (Figure 1 item 7, column 2 lines 19 – 25).

Claim 45 is rejected as applied above in rejecting claim 44. Tso does not explicitly describe a cluster of interconnected computers. Bates teaches that the cluster of devices is a cluster of interconnected personal computers (column 3 lines 38 – 55, column 4 lines 50-55, column 8 lines 16 – 29). The logic for combination is given above in claim 44.

Regarding claim 57, Tso discloses:

A server that attempts to provide encryption services in a client-server environment, comprising:

a communication link to client devices (Figure 1 item 14, column 4 lines 3 – 10);

mass storage for files (Figure 4 item 30, column 5 lines 1 – 43); and

a processor that executes instructions in order to send requested files to the client devices, the instructions also including instructions

(a) to receive a request for a file (Figure 2 item 20, column 2 lines 62 – 67),

(c) to respond to the request by sending the file (Figure 2 item 60, item 70, column 3 lines 1 – 10).

Tso does not explicitly teach means for processing said request at a second location, wherein said means for processing includes means for encrypting said object. Bates teaches "any packets sent by the plugin 29 to virus check controller 44 are encrypted" (column 14 lines 62 – 67). Also, encrypting data objects was well-known in

the art at the time of the Applicant's invention, and it would have been obvious to encrypt the object before sending it over a communications network because, as according to Bates, it would "prevent a malicious party from attempting to corrupt the...information" (column 15 lines 1 – 8).

Claim 59 is rejected as applied above in rejecting claim 57. Furthermore, Tso discloses:

A server as in claim 57, wherein the request is received from and the file is sent to a client device (Figure 2 item 60, item 70, column 3 lines 1 – 10).

Claim 60 is rejected as applied above in rejecting claim 57. Furthermore, Tso discloses: A server as in claim 57, wherein the server is a web server (Figure 1 item 7, column 2 lines 19 – 25).

Claim 61 is rejected as applied above in rejecting claim 57. Furthermore, Tso discloses:

A server as in claim 57. Tso does not explicitly teach that the encrypting device is one of a cluster of devices connected to the server that function similarly to the encrypting device. Bates teaches a virus-scanning environment wherein the scanning device is one of a cluster of scanning devices that can be used to scan for viruses (column 3 lines 38 – 55, column 4 lines 50-55, column 8 lines 16 – 29). Both Bates and Tso pertain to methods of virus scanning and reporting and are therefore analogous arts. Bates states that using multiple computers permits "the responsibility for generating virus status information, as well as the processing horsepower required to

generate the virus status information, to be allocated among the multiple computers" (column 3 lines 38 – 55). Further, Bates states, "by distributing the virus checking responsibilities in this manner, a comparatively greater volume of virus status information may be generated and/or the timeliness of updates to existing virus status information may be improved" (column 3 lines 51 – 55). Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Tso with the cluster of virus scanning devices of Bates to achieve the benefits of reduction of processing power at the scanning device, diversifying the source of virus status information, and as a result, increasing the timeliness of virus status information and the volume of virus status information.

Claim 62 is rejected as applied above in rejecting claim 61. Tso does not explicitly describe a cluster of interconnected computers. Bates teaches that the cluster of devices is a cluster of interconnected personal computers (column 3 lines 38 – 55, column 4 lines 50-55, column 8 lines 16 – 29). The logic for combination is given above in claim 61.

Regarding claim 74, Tso discloses:

Storage containing information including instructions, the instructions executable by a processor to attempt to provide virus protection in a client-server environment, the instructions comprising the steps of:

receiving a request at a server for a file (Figure 2 item 20, column 2 lines 62 - 67);

sending, from the server, an identifier for the file to a cluster of scanning devices that scan the file for viruses (Figure 2 item 40, column 2 lines 38 – 44, column 3 lines 1 - 10),

receiving, at the server, an indication from the scanning devices as to whether or not the file is safe to send from the server (Figure 3 item 200, column 3 lines 48 – 54); and

responding to the request by sending the file if the indication is that the file is safe to send (Figure 2 item 60, item 70, column 3 lines 1 – 10).

Tso does not explicitly disclose that the communication between the server and the cluster of scanning devices is performed using non-uniform memory access. . Bates teaches a virus-scanning environment wherein the scanning device is one of a cluster of scanning devices that can be used to scan for viruses (column 3 lines 38 – 55, column 4 lines 50-55, column 8 lines 16 – 29). It was well-known in the art that NUMA-like performance can be achieved using clusters, with nodal latency being the only issue. However, NUMA is a memory architecture that is commonly used in multiprocessors like the ones used in the cited prior art Bates. However, it was well-known at the time of invention that the NUMA architecture overcomes scalability issues when many CPU's are involved. Therefore, it would have been obvious to use the NUMA architecture in the cluster architecture of Bates to reduce the number of CPUs competing for access to

a shared memory bus, and henceforth, increasing the speed that each of the packets are processed.

Claim 75 is rejected as applied above in rejecting claim 74. Furthermore, Tso discloses:

Storage as in claim 74, wherein the scanning devices indicate that the file is safe to send if the scanning devices determine that the file is not infected with any viruses (Figure 3 item 200, column 3 lines 48 – 54).

Claim 76 is rejected as applied above in rejecting claim 74. Furthermore, Tso discloses:

Storage as in claim 74, wherein the request is received from and the file is sent to a client device (Figure 2 item 60, item 70, column 3 lines 1 – 10).

Claim 77 is rejected as applied above in rejecting claim 74. Furthermore, Tso discloses:

Storage as in claim 74, wherein the server is a web server (Figure 1 item 7, column 2 lines 19 – 25).

Claim 79 is rejected as applied above in rejecting claim 74. Tso does not explicitly describe a cluster of interconnected computers. Bates teaches that the cluster of devices is a cluster of interconnected personal computers (column 3 lines 38 – 55, column 4 lines 50-55, column 8 lines 16 – 29). The logic for combination is given above in claim 78.

Regarding claim 91, Tso discloses:

Storage containing information including instructions, the instructions executable by a processor to operate a filer, the instructions comprising the steps of:

receiving at a first location a request from a user for an object (Figure 2 item 20, column 2 lines 62 - 67);

responding to said request, wherein said step of responding includes delivery of a response to said user (Figure 2 item 60, item 70, column 3 lines 1 – 10).

Tso does not explicitly teach processing said request at a second location, wherein said step of processing includes encrypting said object. Bates teaches "any packets sent by the plugin 29 to virus check controller 44 are encrypted" (column 14 lines 62 – 67). Also, encrypting data objects was well-known in the art at the time of the Applicant's invention, and it would have been obvious to encrypt the object before sending it over a communications network because, as according to Bates, it would "prevent a malicious party from attempting to corrupt the...information" (column 15 lines 1 – 8).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KA
1/04/05

EMMANUEL L. MOISE
PRIMARY EXAMINER